David Cock

August 25, 2014

National ICT Australia (NICTA)
Level 4, 223 Anzac pde.
Kensington NSW
2052 Australia

Telephone, work: +61 2 8306 0486
Telephone, mobile: +61 407 487 919
davec@cse.unsw.edu.au

Education

2014 *PhD, University of New South Wales & National ICT Australia*

"Leakage in Trustworthy Systems", supervisor Gernot Heiser, software systems research group (SSRG).

2005–2009 *PhD-track Research Engineer, National ICT Australia*

L4.verified & seL4 projects, supervisor Gerwin Klein.

2004 *BSc (Hons), University of New South Wales*

Mathematics & Computer Science, major in Systems and Algebra.

Research Experience

The L4.verified project[1] produced the first full correctness proof of a general-purpose operating system (micro-)kernel: seL4[2] (Derrin et al., 2006; Klein et al., 2009, 2010). I was the principal author of the final implementation, which achieved the fastest IPC (inter-process communication) operations ever published on the ARM architecture. The nondeterministic, monadic refinement framework used for the proof was described in Cock et al. (2008).
Roughly 10% of both the C code of seL4, and of the lines of proof script dealt with packed structure manipulation, and were automatically generated (Winwood et al., 2009), using a custom DSL (domain-specific language) compiler (Cock, 2008), which co-generates Isabelle/HOL proof script.
My high-performance, retargetable CPU/system simulator, Lyrebird (Cock, 2010), provided a prototyping platform with an automatically-generated formal model.
My thesis (Cock, 2014a) dealt with the detection and mitigation of covert and side channels in component systems. We developed techniques for detecting, modelling and mitigating compromising channels in security-critical software, in particular both the empirical evaluation of hardware-based channel capacity, and the formal verification of probabilistic security properties (Cock, 2011, 2013, 2014b).
My published formalisation of the probabilistic programming logic/refinement framework pGCL(Cock, 2012) was used to machine check these proofs, and has since been accepted to the archive of formal proofs(Cock, 2014c).

Teaching Experience

[1] http://www.ertos.nicta.com.au/research/l4.verified/
[2] http://ssrg.nicta.com.au/projects/seL4/

2009–2014 *Tutor, Operating Systems and Advanced Operating Systems courses, UNSW*

Small-group instruction of both undergraduate and postgraduate students, and marking duties. Individual guidance and assessment for advanced student projects.

2002–2004 *Consultant & Replacement Tutor, Higher Computing 1A, UNSW*

Individual tuition and guidance for first-year undergraduate students, and supervision of advanced student projects.

Industrial Experience

2005–2014 *Computer Support Officer, National ICT Australia.*

Technical and performance-optimisation support for the automated regression testing of large mechanised proofs. Resource planning and equipment acquisition.

2003–2005 *Programmer, Brain Resource Pty. Ltd.*[a]

Developed a clinical electroencephalogram acquisition system. Development was primarily in Python and C, on a customised Debian distribution. This system was deployed worldwide.
This system included a customised low-latency audio driver, with experimentally-verified jitter bounds.

[a] `http://www.brainresource.com/`

Seminars & Presentations

2014

- "From probabilistic operational semantics to information theory", 5th Conference on Interactive Theorem Proving, Vienna, Austria.
- "How to navigate the literature", NICTA SSRG PhD student boot camp, UNSW, Sydney, Australia.
- "Measuring and Mitigating Side Channels", NICTA software systems summer school, Sydney, Australia.

2013

- "Practical Probability — Applying pGCL to Lattice Scheduling", 4th Conference on Interactive Theorem Proving, Rennes, France.
- "Measuring and Mitigating Side Channels", Systems Group, ETH, Zürich, Switzerland.
- "Measuring and Mitigating Side Channels", Dependable Systems Lab, EPFL, Lausanne, Switzerland.
- "Lyrebird — A Retrospective", Cambridge Computer Laboratory, Cambridge, UK.

2012
- "Verifying Probabilistic Correctness in Isabelle with pGCL", 7th Systems Software Verification Conference, Sydney, Australia.

2011
- "Exploitation as Inference", 4th Workshop on Artificial Intelligence and Security, Chicago, USA.

2010
- "Lyrebird — assigning meanings to machines", 5th Systems Software Verification Conference, Vancouver, Canada.

Grants & Awards

2009–2013 *Australian Postgraduate Award*

A competitive federally-funded full scholarship for research students.

2009–2013 *NICTA Research Project Award*

A competitive scholarship for students undertaking project work at NICTA.

2009–2013 *UNSW Engineering Top-Up Scholarship*

Limited numbers offered annually, awarded for teaching work.

2013 *APSys 2013 Student travel grant.*

2009 *SOSP 2009 Student travel grant.*

Scientific Engagement

Journal Reviewing

- Elsevier—Science of Computer Programming

Conference/Workshop Reviewing

- Springer LNCS—European Symposium on Programming, International Symposium on Formal Methods, Security Proofs for Embedded Systems, International Symposium on Automated Technology for Verification and Analysis
- USENIX—Symposium on Operating System Design and Implementation
- Elsevier—Information and Communication (GandALF 2013)
- IEEE—Real-Time and Embedded Technology and Applications Symposium

References

Gernot Heiser
Senior Principle Researcher, National ICT Australia
Telephone: +61 2 8306 0550
gernot@nicta.com.au

Gerwin Klein Telephone: +61 2 8306 0578
Senior Principal Researcher, National ICT Australia Gerwin.Klein@nicta.com.au
Kevin Elphinstone Telephone: +61 2 8306 0573
Senior Researcher, National ICT Australia Kevin.Elphinstone@nicta.com.au

Publications

David Cock. Bitfields and tagged unions in C: Verification through automatic generation. In Bernhard Beckert and Gerwin Klein, editors, *Proceedings of the 5th International Verification Workshop*, volume 372 of *CEUR Workshop Proceedings*, pages 44–55, Sydney, Australia, August 2008.

David Cock. Lyrebird – assigning meanings to machines. In Gerwin Klein, Ralf Huuck, and Bastian Schlich, editors, *Proceedings of the 5th Systems Software Verification*, pages 1–9, Vancouver, Canada, October 2010. USENIX.

David Cock. Exploitation as an inference problem. In *Proceedings of the 4th ACM Workshop on Artificial Intelligence and Security*, pages 105–106, Chicago, IL, USA, October 2011. doi:10.1145/2046684.2046702.

David Cock. Verifying probabilistic correctness in Isabelle with pGCL. In *Proceedings of the 7th Systems Software Verification*, pages 1–10, Sydney, Australia, November 2012. doi:10.4204/EPTCS.102.15.

David Cock. Practical probability: Applying pGCL to lattice scheduling. In *Proceedings of the 4th International Conference on Interactive Theorem Proving*, pages 1–16, Rennes, France, July 2013. doi:10.1007/978-3-642-39634-2_23.

David Cock. *Leakage in Trustworthy Systems*. Phd thesis, Computer Science and Engineering, Sydney, Australia, August 2014a.

David Cock. From probabilistic operational semantics to information theory - side channels with pGCL in isabelle. In *Proceedings of the 5th International Conference on Interactive Theorem Proving*, pages 1–15, Vienna, Austria, July 2014b. Springer.

David Cock. pGCL for Isabelle. *Archive of Formal Proofs*, July 2014c. `http://afp.sf.net/entries/pGCL.shtml`, Formal proof development.

David Cock, Gerwin Klein, and Thomas Sewell. Secure microkernels, state monads and scalable refinement. In Otmane Ait Mohamed, Csar Muoz, Sone Tahar, editor, *Proceedings of the 21st International Conference on Theorem Proving in Higher Order Logics*, pages 167–182, Montreal, Canada, August 2008. Springer. doi:10.1007/978-3-540-71067-7_16.

Philip Derrin, Kevin Elphinstone, Gerwin Klein, David Cock, and Manuel M. T. Chakravarty. Running the manual: An approach to high-assurance microkernel development. In *Proceedings of the ACM SIGPLAN Haskell Workshop*, Portland, OR, USA, September 2006. doi:10.1145/1159842.1159850.

Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. seL4: Formal verification of an OS kernel. In *Proceedings of the 22nd ACM Symposium on Operating Systems Principles*, pages 207–220, Big Sky, MT, USA, October 2009. ACM. doi:10.1145/1629575.1629596.

Gerwin Klein, June Andronick, Kevin Elphinstone, Gernot Heiser, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. seL4: Formal verification of an operating system kernel. *Communications of the ACM*, 53(6):107–115, June 2010. doi:10.1145/1743546.1743574.

Simon Winwood, Gerwin Klein, Thomas Sewell, June Andronick, David Cock, and Michael Norrish. Mind the gap: A verification framework for low-level C. In Stefan Berghofer, Tobias Nipkow, Christian Urban, and Makarius Wenzel, editors, *Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics*, volume 5674 of *Lecture Notes in Computer Science*, pages 500–515, Munich, Germany, August 2009. Springer-Verlag. doi:10.1007/978-3-642-03359-9_34.